Secureworks®

Threat Intelligence Executive Report

Volume 2022, Number 5

Presented by the Counter Threat Unit™ (CTU) research team

Executive Summary

The Secureworks® Counter Threat Unit™ (CTU) research team analyzes security threats to help organizations protect their systems. During July and August, CTU™ researchers identified the following noteworthy issues and changes in the global threat landscape:

- Ransomware groups leave tell-tale traces
- Government-sponsored threat groups target intellectual property
- Infostealers are more than a minor nuisance

Ransomware groups leave tell-tale traces

The faster a ransomware threat actor can move from initial access to encryption, the less time there is to detect and stop the attack. Just like most people under pressure, cybercriminals often turn to techniques that they can trust.

There are three main types of threat actors in the ransomware-as-a-service (RaaS) ecosystem: operators, affiliates, and initial access brokers. Although media coverage usually focuses on the operators, monitoring the activities of all three types provides useful threat intelligence about their techniques, tactics, and procedures (TTPs) and helps stop attacks before they succeed.

In July, CTU researchers investigated four network intrusions carried out by GOLD MATADOR, a financially motivated cybercriminal threat group that operates as an affiliate of GOLD HAWTHORNE's Hive ransomware program. The researchers observed that once the threat actors obtained initial access to victims' systems, they used similar TTPs across the intrusions.

CTU researchers also observed an attack by initial access broker GOLD MELODY (also known as Prophet Spider) that used well-known TTPs, enabling rapid detection and alerting. As a result, the victim was able to limit the spread of the attack by isolating the compromised host from the network and initiating incident response.

These incidents highlight the importance of comprehensively monitoring all endpoints, networks, and cloud-based assets for activity indicative of an imminent ransomware deployment. Attacks were rapidly detected and foiled because of comprehensive monitoring from an extended detection and response (XDR) solution. Successful attacks occurred in networks with partial or no XDR implementation. In one incident, initial access to ransomware deployment took just 18 hours. Dwell times are often shorter. Being aware of and able to detect frequently used TTPs is essential.

What you should do next:
Implement an XDR solution on every server, endpoint, network, and cloud resource. Detect known TTPs belonging to all types of ransomware threat actors.

Government-sponsored threat groups target intellectual property

Attackers in search of intellectual property can maintain a presence on a compromised network for months at a time and may return on regular occasions. Detecting this unwanted presence at the outset is crucial.

CTU researchers analyzed an attack during which the threat actor targeted intellectual property related to the organization's advanced technology. Tools and tactics used during the attack pointed to a Chinese government-sponsored threat actor. The threat actor likely first obtained access to the victim's network in November 2021. They then returned on several occasions to conduct discovery and reconnaissance, using tools to maintain their access. On their final visit, they were able to use these insights and tools to move laterally and swiftly compromise a server containing sensitive data.

Intellectual property theft is one of the main reasons that government-sponsored threat actors target commercial organizations. Any organization owning intellectual property that might be of economic value to other countries is a potential target. During the early phases of the COVID-19 pandemic, pharmaceutical companies conducting research and development were attractive targets.

Countries with a known record of intellectual property theft include China, Russia, North Korea, and Iran. China in particular conducts attacks of this nature, stealing from organizations in developed or competing economies to support its own economic and military development. The ransomware attacks attributed to the Chinese BRONZE STARLIGHT threat group are likely covers for intellectual property theft and cyberespionage. Cybercriminals may also target intellectual property in data extortion attacks.

An organization wanting to protect itself against intellectual property theft must identify relevant assets and how they are stored on the network. Comprehensive monitoring is also essential to detect suspicious network activity, including data exfiltration.

What you should do next:
Audit your systems to ensure that intellectual property and other valuable data assets are not stored on systems that are visible to the internet. Consider network segmentation to place additional barriers in the way of network intruders.

Infostealers are more than a minor nuisance

Threat actors employ many types of malware before deploying ransomware. Being able to detect malware such as infostealers can provide important opportunities for early remediation.

It's not surprising that organizations view ransomware deployment as the main event in ransomware attacks. However, other types of malware have major supporting roles. Being able to detect them plays an important part in stopping ransomware attacks from taking place. Infostealers (or information stealers) are one type of supporting malware. Threat actors use them to target and steal browser data such as usernames, passwords, cookies, authentication tokens, VPN data, chat application data, extension data, stored credit card information, and cryptocurrency wallets.

During July and August, CTU researchers obtained the source code and samples of a new cross-platform infostealer dubbed Luca that has been widely promoted on underground markets and is designed to be difficult to detect and analyze. They observed the well-established RedLine infostealer, used by threat actors since at least March 2020, used in a spam email campaign. Weeks earlier, the researchers discovered over two million infostealer logs for sale on an underground forum on a single day.

Although infostealers have historically been disregarded as nuisance malware rather than a serious threat, they pose a growing risk to organizations' credentials and data. Stolen credentials give threat actors network access that they could translate into successful ransomware attacks. The presence of infostealers on an organization's network should not be overlooked in risk calculations or mitigation activity. Detecting and removing infostealers from networks is an essential early step in stopping ransomware.

What you should do next:
Check that your monitoring and detection systems can detect widely used infostealer malware. Fully implement multi-factor authentication to reduce the utility of stolen credentials.

Conclusion

Whether a threat actor aims to maintain persistence on a system over a long period of time or conduct a quick but devastating ransomware attack, they may use many types of malware before or during the attack. That means organizations have multiple opportunities to detect threat actor activity. Comprehensive implementation of extended monitoring and detection systems is an essential part of protecting an organization's data and other assets.

A glance at the CTU research team

CTU researchers frequently serve as expert resources for the media, publish technical analyses for the security community, and speak about emerging threats at security conferences. Leveraging Secureworks' advanced security technologies and a network of industry contacts, the CTU research team tracks threat actors and analyzes anomalous activity, uncovering new attack techniques and threats. This process enables CTU researchers to identify threats as they emerge and develop countermeasures that protect customers before damage can occur.

Research

Understanding the nature of threats customers face, and creating countermeasures to address and protect.

Intelligence

Providing information that extends the visibility of threats beyond the edges of a network.

Integration

Infusing CTU research and intelligence into Secureworks managed security services and security consulting practices.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world. We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
www.secureworks.com

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs Forest, Sydney NSW Australia 2086

Japan
Otemachi One Tower 17F, 2-1,
Otemachi 1-chome, Chiyoda-ku,
Tokyo 100-8159,
Japan
www.secureworks.jp

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom

1 Tanfield
Edinburgh EH3 5DA
United Kingdom

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111

If you need immediate assistance, call our 24x7 **Global Incident Response Hotline:**

+1-770-870-6343

